

09/05/00

UTILITY
PATENT APPLICATION
TRANSMITTAL(Only for new nonprovisional applications
under 37 CFR 1.53(b))

Title of Invention

UNDENIABLE DIGITAL SIGNATURE SCHEME
BASED ON QUADRATIC FIELD

Named Inventor(s)

TSUYOSHI TAKAGI;
INGRID BIEHL;
SACHAR PAULUS

Attorney Docket

13700-0251

Express Mail Label No.

EL561430943US

JC836 U.S. PTO
09/05/00

APPLICATION ELEMENTS

1. ☒ Fee Transmittal Form
(Submit an original, and a duplicate for fee processing)
2. ☒ Specification, Claims,
and Abstract Total Pages 39
3. ☒ Drawings Total Sheets 8
4. Oath or Declaration Total Pages 2
 - a. ☒ Newly executed (original or copy)
 - b. ☐ Copy from prior application (37 CFR 1.63(d))
(for continuation/divisional with Box 17
completed)
[Note Box 5 Below]
(i) ☐ DELETION OF INVENTOR(S)
Signed statement attached
deleting inventor(s) named in the
prior application, see 37 CFR
1.63(d)(2) and 1.33(b).
5. ☐ Incorporation by Reference
(usable if Box 4b is checked)
The entire disclosure of the prior application, from
which a copy of the oath or declaration is supplied
under Box 4b, is considered as being part of the
disclosure of the accompanying application and is
hereby incorporated by reference therein.
6. ☐ Microfiche Computer Program (Appendix)
7. ☐ Nucleotide and/or Amino Acid Sequence
Submission (if applicable, all necessary)
 - a. ☐ Computer Readable Copy
 - b. ☐ Paper Copy (identical to computer copy)
 - c. ☐ Statement verifying identity of
above copies

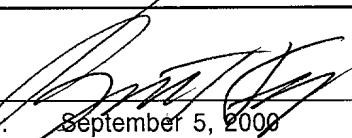
Assistant Commissioner for Patents
ADDRESS TO: Box Patent Application
Washington, D.C. 20231

ACCOMPANYING APPLICATION PARTS

8. ☒ Assignment:
 - a. ☒ Assignment Papers (cover sheet &
document(s))
 - b. ☐ Assignment is of record in parent
application No. _____
9. ☐ 37 CFR 3.73(b) Statement
(when there is an assignee)
☐ Power of Attorney by assignee
10. ☐ English Translation Document (if applicable)
11. ☐ Information Disclosure Statement (IDS)
PTO-1449
☐ Copies of IDS Citations
12. ☐ Preliminary Amendment
13. ☒ Return Receipt Postcard (MPEP 503)
(Should be specifically itemized)
14. ☐ Small Entity Statement(s)
☐ Statement filed in prior application
Status still proper and desired
15. ☐ Certified Copy of Priority Document(s)
16. ☐ Other: _____

17. If a **CONTINUING APPLICATION**, check appropriate box and supply the requisite information:
☐ Continuation ☐ Divisional ☐ Continuation-in-part (CIP) of prior application No:
Recite complete dependency back to first parent application: _____

18. CORRESPONDENCE ADDRESS:

Roger T. Frost
KILPATRICK STOCKTON LLP
2400 Monarch Tower
3424 Peachtree Road, N.E.
Atlanta, Georgia 30326By:  Reg. No. 22,176
Date: September 5, 2000
Telephone: 404-949-2400
Facsimile: 404-949-2499

UNDENIABLE DIGITAL SIGNATURE SCHEME
BASED ON QUADRATIC FIELD

5 BACKGROUND OF THE INVENTION

FIELD OF THE INVENTION

The present invention relates to an undeniable digital
signature scheme which is a type of digital signature that
10 can protect a privacy of a signer.

DESCRIPTION OF THE BACKGROUND ART

In electronic communications, the digital signature
technology is effective in checking the validity of data.
15 The most widely used digital signature is the RSA signature
that utilizes modular exponentiation calculations (see R.
Rivest, A. Shamir and L.M. Adleman, "A method for obtaining
digital signatures and public key cryptosystems",
Communications of ACM, 21(2), pp. 120-126, 1978).

20 A digital signature scheme is evaluated by its
security and its signature generation/verification speed,
so that a digital signature scheme with a higher security
and a faster computation speed is considered as superior.
The security of the RSA signature is based on the
25 intractability to compute the secret keys from public keys.
A more secure system can be realized by making the key
length of the public key longer. The RSA signature involves
the modular exponentiation calculations that have great
computational complexity so that there has been a drawback
30 that the signature generation/verification requires a
considerable amount of time.

As a variation of the digital signature, there has
been a proposition of an undeniable signature (see D. Chaum
and H. van Antwerpen, "Undeniable Signatures", Advances in
35 Crypttology - CRTPTO'89, LNCS 435, pp. 212-216, Springer-

Verlag, 1990). In the undeniable signature scheme, the legitimacy of the signature cannot be verified without communicating with a signer, so that the signature can be traced and the privacy of the signer can be protected. A
5 standard application of the undeniable signature is a secure distribution of software, where a purchaser of the software can make a contact with a distributor who is also a signer and check that the software does not contain a virus entered by a third person.

10 The most efficient undeniable signature scheme to date is the RSA-based undeniable signatures (see R. Gennaro, H. Krawczyk and T. Rabin, "RSA-Based Undeniable Signatures", Advances in Cryptology - CRYPTO '89, LNCS 435, pp. 212-216, Springer-Verlag, 1990). This scheme is based on the RSA
15 signature so that it is also associated with the problem of a large computational complexity.

In this regard, a smartcard has been attracting much attentions lately as an easily portable device for storing secret keys securely. However, a smartcard has limited
20 computational resources so that a considerable time would be required to execute the RSA-based undeniable signature scheme on a smartcard. Moreover, in the case of using the undeniable signatures in a large scale information distribution system, there arises a problem of overloading
25 the server. For these reasons, there has been demands for an efficient and high speed undeniable signature scheme.

SUMMARY OF THE INVENTION

30

It is therefore an object of the present invention to provide an undeniable digital signature scheme which is far more efficient compared with the conventional RSA-based undeniable signature scheme, and which is capable of
35 resolving the problems associated with the conventional

RSA-based undeniable signatures.

According to one aspect of the present invention there is provided a method of undeniable digital signature, comprising the steps of: (a) generating public keys (D, P, k, t) and secret keys (D1, q) at a signer side, by generating two primes p, q ($p, q > 4$, $p \equiv 3 \pmod{4}$, $\sqrt{p/3} < q$), computing $D1 = -p$ and $D = D1q^2$, obtaining a bit length k of $\sqrt{|D1|}/4$ and a bit length t of $q - (D1/q)$ where $(D1/q)$ denotes Kronecker symbol, and generating a kernel element P of a map from a class group $Cl(D)$ to a class group $Cl(D1)$; (b) generating a signature S for a message m at the signer side, by embedding the message m into a message ideal M in the class group $Cl(D)$ where a norm of the message ideal M is larger than k+1 bits, and mapping the message ideal M to the class group $Cl(D1)$ and pulling the mapped message ideal M back to the class group $Cl(D)$; and (c) verifying the signature S by: (c1) checking whether a norm $N(S)$ of the signature S is smaller than k bits or not, and judging that the signature S is illegal when the norm $N(S)$ is larger than k bits, or generating a challenge C when the norm $N(S)$ is not larger than k bits, by computing the message ideal M of the message m, generating a random integer r smaller than t bits, computing $H = (M/S)^r$, generating a random ideal B whose norm is smaller than k-1 bits, and computing the challenge $C = BH$, at a verifier side; (c2) computing a response W by mapping the challenge C to the class group $Cl(D1)$ and pulling the mapped challenge C back to the class group $Cl(D)$ and squaring a result of mapping and pulling back, using the secret keys (D1, q), at the signer side; and (c3) checking whether $W = B^2$ holds or not, and judging that the signature S is legal when $W = B^2$ holds or that the signature S is illegal otherwise, at the verifier side.

According to another aspect of the present invention there is provided a signer device for processing an undeniable digital signature, comprising: a key generation

unit for generating public keys (D, P, k, t) and secret keys $(D1, q)$, by generating two primes p, q ($p, q > 4, p = 3 \bmod 4, \sqrt{p/3} < q$), computing $D1 = -p$ and $D = D1q^2$, obtaining a bit length k of $\sqrt{|D1|}/4$ and a bit length t of $q - (D1/q)$ where $(D1/q)$ denotes Kronecker symbol, and
5 generating a kernel element P of a map from a class group $Cl(D)$ to a class group $Cl(D1)$; a signature generation unit for generating a signature S for a message m , by embedding the message m into a message ideal M in the class group
10 $Cl(D)$ where a norm of the message ideal M is larger than $k+1$ bits, and mapping the message ideal M to the class group $Cl(D1)$ and pulling the mapped message ideal M back to the class group $Cl(D)$; and a response generation unit for receiving a challenge $C = BH$ from a verifier side, where B
15 is a random ideal whose norm is smaller than $k-1$ bits, $H = (M/S)^r$, and r is a random integer smaller than t bits, computing a response W by mapping the challenge C to the class group $Cl(D1)$ and pulling the mapped challenge C back to the class group $Cl(D)$ and squaring a result of mapping
20 and pulling back, using the secret keys $(D1, q)$, and sending the response W to the verifier side, in a process for verifying the signature S .

According to another aspect of the present invention there is provided a verifier device for processing an
25 undeniable digital signature, using a message m and a signature S received from a signer side, where public keys (D, P, k, t) and secret keys $(D1, q)$ are defined by generating two primes p, q ($p, q > 4, p = 3 \bmod 4, \sqrt{p/3} < q$), computing $D1 = -p$ and $D = D1q^2$, obtaining a bit length
30 k of $\sqrt{|D1|}/4$ and a bit length t of $q - (D1/q)$ where $(D1/q)$ denotes Kronecker symbol, and generating a kernel element P of a map from a class group $Cl(D)$ to a class group $Cl(D1)$, and the signature S for the message m is generated by embedding the message m into a message ideal M in the class
35 group $Cl(D)$ where a norm of the message ideal M is larger

than $k+1$ bits, and mapping the message ideal M to the class group $Cl(D_1)$ and pulling the mapped message ideal M back to the class group $Cl(D)$, the verifier device comprising: a norm checking unit for checking whether a norm $N(S)$ of the signature S is smaller than k bits or not, and judging that the signature S is illegal when the norm $N(S)$ is larger than k bits; a challenge generation unit for generating a challenge C when the norm $N(S)$ is not larger than k bits, by computing the message ideal M of the message m , generating a random integer r smaller than t bits, computing $H = (M/S)^r$, generating a random ideal B whose norm is smaller than $k-1$ bits, and computing a challenge $C = BH$, and for sending the challenge C to a signer side; and a response checking unit for receiving a response W from the signer side, checking whether $W = B^2$ holds or not, and judging that the signature S is legal when $W = B^2$ holds or that the signature S is illegal otherwise, where the response W being obtained by mapping the challenge C to the class group $Cl(D_1)$ and pulling the mapped challenge C back to the class group $Cl(D)$ and squaring a result of mapping and pulling back, using the secret keys (D_1, q) .

According to another aspect of the present invention there is provided a computer usable medium having computer readable program codes embodied therein for causing a computer to function as a signer device for processing an undeniable digital signature, the computer readable program codes including: a first computer readable program code for causing said computer to generate public keys (D, P, k, t) and secret keys (D_1, q) , by generating two primes p, q ($p, q > 4, p \equiv 3 \pmod{4}, \sqrt{p/3} < q$), computing $D_1 = -p$ and $D = D_1q^2$, obtaining a bit length k of $\sqrt{|D_1|}/4$ and a bit length t of $q - (D_1/q)$ where (D_1/q) denotes Kronecker symbol, and generating a kernel element P of a map from a class group $Cl(D)$ to a class group $Cl(D_1)$; a second computer readable program code for causing said computer to generate a

signature S for a message m, by embedding the message m into a message ideal M in the class group $Cl(D)$ where a norm of the message ideal M is larger than $k+1$ bits, and mapping the message ideal M to the class group $Cl(D_1)$ and
5 pulling the mapped message ideal M back to the class group $Cl(D)$; and a third computer readable program code for causing said computer to receive a challenge $C = BH$ from a verifier side, where B is a random ideal whose norm is smaller than $k-1$ bits, $H = (M/S)^r$, and r is a random
10 integer smaller than t bits, compute a response W by mapping the challenge C to the class group $Cl(D_1)$ and pulling the mapped challenge C back to the class group $Cl(D)$ and squaring a result of mapping and pulling back, using the secret keys (D_1, q) , and send the response W to
15 the verifier side, in a process for verifying the signature S.

According to another aspect of the present invention there is provided a computer usable medium having computer readable program codes embodied therein for causing a
20 computer to function as a verifier device for processing an undeniable digital signature, using a message m and a signature S received from a signer side, where public keys (D, P, k, t) and secret keys (D_1, q) are defined by generating two primes p, q ($p, q > 4$, $p \equiv 3 \pmod{4}$, $\sqrt{p/3} <$
25 q), computing $D_1 = -p$ and $D = D_1q^2$, obtaining a bit length k of $\sqrt{|D_1|}/4$ and a bit length t of $q - (D_1/q)$ where (D_1/q) denotes Kronecker symbol, and generating a kernel element P of a map from a class group $Cl(D)$ to a class group $Cl(D_1)$, and the signature S for the message m is generated by
30 embedding the message m into a message ideal M in the class group $Cl(D)$ where a norm of the message ideal M is larger than $k+1$ bits, and mapping the message ideal M to the class group $Cl(D_1)$ and pulling the mapped message ideal M back to the class group $Cl(D)$, the computer readable program codes
35 including: a first computer readable program code for

causing said computer to check whether a norm $N(S)$ of the signature S is smaller than k bits or not, and judge that the signature S is illegal when the norm $N(S)$ is larger than k bits; a second computer readable program code for
5 causing said computer to generate a challenge C when the norm $N(S)$ is not larger than k bits, by computing the message ideal M of the message m , generating a random integer r smaller than t bits, computing $H = (M/S)^r$, generating a random ideal B whose norm is smaller than $k-1$
10 bits, and computing the challenge $C = BH$, and send the challenge C to a signer side; and a third computer readable program code for causing said computer to receive a response W from the signer side, check whether $W = B^2$ holds or not, and judge that the signature S is legal when $W = B^2$
15 holds or that the signature S is illegal otherwise, where the response W being obtained by mapping the challenge C to the class group $Cl(D1)$ and pulling the mapped challenge C back to the class group $Cl(D)$ and squaring a result of mapping and pulling back, using the secret keys $(D1, q)$.

20 According to another aspect of the present invention there is provided a method for providing a software vending service, comprising the steps of: (a) attaching an undeniable digital signature to a software offered for downloading by clients at a software vendor side, according
25 to an undeniable digital signature scheme based on a quadratic field; and (b) carrying out a process of verifying the undeniable digital signature at the software vendor side interactively with each client which has downloaded the software with the undeniable digital
30 signature attached thereto, so as to prove that the software has not been altered from an original.

According to another aspect of the present invention there is provided a method for enabling a user to check authenticity of an e-commerce/information service provider,
35 comprising the steps of: (a) obtaining public keys, secret

keys, and a signature for the public keys from a
certificate authority at the e-commerce/information service
provider, the signature being generated by the certificate
authority according to an undeniable digital signature
5 scheme; (b) providing the public keys and the signature
from the e-commerce/information service provider to the
user, such that the user carries out a process of verifying
the signature provided from the e-commerce/information
service provider to the user, interactively with the
10 certificate authority to prove authenticity of the public
keys provided by the e-commerce/information service
provider; and (c) receiving an encrypted random data from
the user, the encrypted random data being encrypted by the
user using the public keys, decrypting the encrypted random
15 data using the secret keys, and returning a decrypted
random data to the user, such that the user checks if the
decrypted random data coincides with an original random
data to prove that the e-commerce/information service
provider has authentic secret keys.

20 According to another aspect of the present invention
there is provided a method for enabling a user to check
authenticity of an e-commerce/information service provider,
comprising the steps of: (a) issuing public keys, secret
keys, and a signature for the public keys from a
25 certificate authority to the e-commerce/information service
provider, the signature being generated according to an
undeniable digital signature scheme; and (b) carrying out a
process of verifying the signature provided from the e-
commerce/information service provider to the user, at the
30 certificate authority interactively with the user in order
to prove authenticity of the public keys provided by the e-
commerce/information service provider.

According to another aspect of the present invention
there is provided a method for enabling a user to check
35 authenticity of an e-commerce/information service provider,

comprising the steps of: (a) generating a signature for a hash value of a home page of the e-commerce/information service provider at a certificate authority according to an undeniable digital signature scheme; (b) posting the signature on a display of the home page of the e-commerce/information service provider at a user side from the certificate authority, such that the user can initiate a process of verifying the signature by clicking the signature on the display; and (c) carrying out the process of verifying the signature at the certificate authority interactively with the user in order to prove authenticity of the e-commerce/information service provider.

Other features and advantages of the present invention will become apparent from the following description taken in conjunction with the accompanying drawings.

BRIEF DESCRIPTION OF THE DRAWINGS

Fig. 1 is a table summarizing symbols used in describing a quadratic field that is utilized in the undeniable digital signature scheme according to the present invention.

Fig. 2 is a table summarizing parameters used in the undeniable digital signature scheme according to the present invention.

Fig. 3 is a flow chart showing a processing procedure of the undeniable digital signature scheme according to the present invention.

Fig. 4 is a block diagram showing exemplary configurations of a signer device and a verifier device for carrying out the processing procedure of Fig. 3.

Fig. 5 is a table summarizing a simulation result for comparing efficiency in the undeniable digital signature scheme according to the present invention and the

conventional RSA-type digital signature scheme.

Fig. 6 is a schematic diagram showing an exemplary configuration of an undeniable digital signature system for a software vending service utilizing the undeniable digital signature scheme according to the present invention.

Fig. 7 is a block diagram showing an exemplary configuration of an authentication server in the undeniable digital signature system of Fig. 6.

Fig. 8 is a schematic diagram showing an exemplary configuration of an undeniable digital signature system for an e-commerce service utilizing the undeniable digital signature scheme according to the present invention.

Fig. 9 is a schematic diagram showing an exemplary configuration of an undeniable digital signature system for a news/mail providing service utilizing the undeniable digital signature scheme according to the present invention.

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENTS

Referring now to Fig. 1 to Fig. 9, one embodiment of the undeniable digital signature scheme according to the present invention will be described in detail.

The undeniable digital signature scheme of the present invention utilizes a structure of the class group of a quadratic field, especially fast algorithms for switching between the maximal order and the non-maximal order.

First, the property of a quadratic field utilized in this undeniable digital signature scheme will be summarized briefly.

Let p and q be two prime numbers greater than four that are given by $p \equiv 3 \pmod{4}$ and $\sqrt{p/3} < q$, and define $D_1 = -p$ and $D = D_1 q^2$, where D_1 is a fundamental discriminant, D is a non-fundamental discriminant, and q is a conductor.

Denoting the integer ring by Z , $O_D = Z + (D+\sqrt{D})/2Z$ gives a quadratic order with discriminant D . The class group with discriminant D will be denoted as $Cl(D)$. An ideal A in the class group $Cl(D)$ is represented by $A = (a, b)$ where "a" is
5 a positive integer and "b" is an integer satisfying $b^2 \equiv D \pmod{4a}$. If $-a < b \leq a$ and $|b| \leq a \leq c = (b^2 - D)/4a$, and assuming that $b \geq 0$ when $a = c$ or $a = |b|$, then (a, b) can be uniquely determined for the ideal A . A norm of the ideal A will be denoted as $N(A) = a$ where $A = (a, b)$. The
10 definitions of various symbols described above are summarized in a table shown in Fig. 1.

In the undeniable digital signature scheme of the present invention, there is a need to compute the modular exponentiation A^r of an ideal A in the class group $Cl(D)$.
15 For this computation of the modular exponentiation A^r , it is possible to utilize the algorithms called "Multiply", "Square" and "Reduce" or their variant called "Square & Multiply" as disclosed in J. Buchmann, S. Duellmann and H.C. Williams, "On the complexity and efficiency of a new
20 key exchange system", Advances in Cryptology - CRYPTO '89. LNCS 434, pp. 597-616, Springer-Verlag, 1990, or the algorithms called "NUCOMP" and "NUDUPL" as disclosed in D. Shanks, "On Gauss and Composition I, II", NATO ASI on Number Theory and Applications (R.A. Mollin, editor), pp.
25 163-204, Kluwer Academic Press, 1989.

Also, in the undeniable digital signature scheme of the present invention, the switching map between the class group of maximal order $Cl(D_1)$ and the class group of non-maximal order $Cl(D)$ plays an important role. The
30 computations for this switching map only involve easy calculations such as that of the greatest common divisor so that they can be done very fast. For this switching map, it is possible to utilize the algorithms called "GoToMaxOrder" and "GoToNonMaxOrder" as disclosed in D. Huehnlein, M.J. Jacobson, Jr., S. Paulus and T. Takagi, "A cryptosystem
35

based on non-maximal imaginary quadratic orders with fast decryption", Advances in Cryptology - EUROCRYPT '98, LNCS 1403, pp. 294-307, Springer-Verlag, 1998.

5 Now, with references to Fig. 2 to Fig. 5, the processing of the undeniable digital signature scheme according to the present invention will be described in detail.

10 Fig. 2 summarizes parameters used in this undeniable digital signature scheme, Fig. 3 shows an overall processing procedure of this undeniable digital signature scheme, and Fig. 4 shows exemplary configurations of a signer device and a verifier device for carrying out the processing procedure of Fig. 3.

15 As shown in Fig. 3, this undeniable digital signature scheme generally comprises three major stages of a key generation (step S10), a signature generation (step S20) and a signature verification (step S30).

20 In the key generation stage, a key generation unit 11 of a signer device 10 carries out the following operation. Namely, two primes p, q ($p, q > 4, p \equiv 3 \pmod{4}, \sqrt{p/3} < q$) are generated, and $D1 = -p$ and $D = D1q^2$ are computed. Then, a bit length k of $\sqrt{|D1|}/4$ and a bit length t of $q - (D1/q)$ where $(D1/q)$ denotes Kronecker symbol, are obtained. Also, 25 a kernel element P of the map from the class group $Cl(D)$ to the class group $Cl(D1)$ is generated using the algorithm "KERNEL" described below. Here, the algorithm "KERNEL" is used as an exemplary algorithm to generate a kernel element $P(Cl(D) \rightarrow Cl(D1))$. Then, the public keys are defined as $(D,$ 30 $P, k, t)$ while the secret keys are defined as $(D1, q)$. The public keys (D, P, k, t) and the secret keys $(D1, q)$ so obtained are stored in a key memory unit 12 of the signer device 10.

35 Note that the security of the quadratic field based cryptosystem that underlies this undeniable digital

signature scheme depends on the intractability of calculating D_1 and q from D which is the well known integer factorization problem. For further details, see D.

- 5 Huehnlein, M.J. Jacobson, Jr., S. Paulus and T. Takagi, "A cryptosystem based on non-maximal imaginary quadratic orders with fast decryption", Advances in Cryptology - EUROCRYPT '98, LNCS 1403, pp. 294-307, Springer-Verlag, 1998.

- 10 In the signature generation stage, a signature generation unit 14 of the signer device 10 carries out the following operation. Namely, a message m generated by a message generation unit 13 is embedded into a message ideal $M = (u, b)$ in the class group $Cl(D)$ where a norm of the message ideal M is larger than $k+1$ bits, using the
- 15 algorithm "Embedding" described below. Here, the algorithm "Embedding" is used as an exemplary algorithm to embed a message m into a message ideal M . Then, the signature S for the message ideal M is generated by

- 20
$$S = \text{GoToNonMaxOrder}(\text{GoToMaxOrder}(M))$$

- using the algorithms "GoToMaxOrder" and "GoToNonMaxOrder" described below, so as to obtain a pair (m, S) of the message and the signature. Here, the algorithms
- 25 "GoToNonMaxOrder" and "GoToMaxOrder" are used as exemplary algorithms to map the ideal M to the class group $Cl(D_1)$ of the fundamental discriminant D_1 and to pull the mapped ideal M back to the class group $Cl(D)$ of the non-fundamental discriminant D . This pair (m, S) is then sent
- 30 to the verifier.

The signature verification stage includes the following three steps.

- A verification step I (step S31) is carried out by a norm checking unit 21 and a challenge generation unit 22 of
- 35 a verifier device 20 as follows. First, whether a norm $N(S)$

of the signature is smaller than k bits or not is checked by the norm checking unit 21. If it is larger than k bits, it implies that the signature is illegal. On the other hand, when it is not larger than k bits, the challenge generation unit 22 carries out the following operation. Namely, the message ideal M of the message m is computed using the algorithm "Embedding" described below. Then, a random integer r smaller than t bits is generated, and $H = (M/S)^r$ is computed. Next, a random ideal B whose norm is smaller than $k-1$ bits is generated using the algorithm "Embedding" described below, and $C = BH$ is computed. This C is a challenge that is sent to the signer. Here, the algorithm "Embedding" is used as an exemplary algorithm to generate a random ideal B .

15 A verification step II (step S32) is carried out by a response generation unit 15 of the signer device 10 as follows. Namely, according to the secret keys $(D1, q)$ stored in the key memory unit 12, the response generation unit 15 computes

20

$$W = (\text{GoToNonMaxOrder}(\text{GoToMaxOrder}(C)))^2$$

using the algorithms "GoToMaxOrder" and "GoToNonMaxOrder" described below, and sends this W back to the verifier as a response. Here, the algorithms "GoToNonMaxOrder" and "GoToMaxOrder" are used as exemplary algorithms to map the ideal C to the class group $Cl(D1)$ of the fundamental discriminant $D1$ and to pull the mapped ideal C back to the class group $Cl(D)$ of the non-fundamental discriminant D .

30 A verification step III (step S33) is carried out by a response checking unit 23 of the verifier device 20 as follows. Namely, the response checking unit 23 checks whether $W = B^2$ holds or not. If it holds, then the signature is legal, whereas otherwise the signature is
35 illegal.

It is to be noted that I. Biehl, S. Paulus and T. Takagi, "Efficient Undeniable Signature Schemes based on Ideal Arithmetic in Quadratic Orders", Conference on the Mathematics of Public Key Cryptography, June 1999, also
5 discloses an undeniable digital signature scheme but this scheme is different from the undeniable digital signature scheme of the present invention in that the signature verification stage of this reference uses the Zero-Knowledge Protocol for L_{ker} which is far more complicated
10 and time consuming than the algorithm used in the undeniable digital signature scheme of the present invention.

The algorithm "KERNEL" to generate a kernel element $P(Cl(D) \Rightarrow Cl(D1))$ is as follows.

15

20

25

30

35

Algorithm KERNEL

Input: fundamental discriminant D_1 , conductor q

Output: ideal $P \in (Cl(D) \rightarrow Cl(D_1))$

```

1. /* Generate  $\alpha = (x+y\sqrt{D_1})/2$  */
5   1.1. Generate integers  $x, y$  ( $< \sqrt{D_1}$ )
   2. /* Standard representation of  $\alpha_0 = (A, B)$  */
   2.1. Find integer  $(m, kn)$  such that
        $m = ky+n(x+yD_1)/2$ 
   2.2.  $A \leftarrow |(x^2-y^2D_1)|/4m^2$ 
10  2.3.  $B \leftarrow (kx+n(x+y)D_1/2)/m \bmod 2A, (-A \leq B < A)$ 
   3. /* Compute  $GoToNonMaxOrder(A) = (a, b)$  */
   3.1.  $a \leftarrow A$ 
   3.2.  $b \leftarrow Bq \bmod 2A, (-a \leq b < a)$ 
   4. /* Reduce  $(a, b)$  */
15  4.1.  $c \leftarrow (D-b^2)/4a$ 
   4.2. WHILE  $\{-a < b \leq a < c\}$  or  $\{0 \leq b \leq a = c\}$  DO
       4.2.1. Find  $\mu, \lambda$  such that  $-a \leq \mu = b + 2\lambda a < a$ 
       4.2.2.  $(a, b, c) \leftarrow (c - (b+\mu)\lambda/2, \mu, a)$ 
   4.3. IF  $a=c$  AND  $b < 0$  THEN  $b \leftarrow -b$ 
20  4.4. RETURN  $(a, b)$ 

```

The algorithm "Embedding" to embed a message m into a message ideal M is as follows.

25 Algorithm Embedding

Input: non-fundamental discriminant D ,

message m smaller than k bits

Output: message ideal $M \in Cl(D)$

```

1. Generate  $u$  which is a smallest quadratic residue
30 among prime numbers larger than  $m$ 
   2. Find  $b$  such that  $b^2 \equiv D \bmod 4u, (-u < b \leq u)$ 
   3. RETURN  $M = (u, b)$ 

```

35 The algorithm "GoToNonMaxOrder" and "GoToMaxOrder" to map the ideal to the class group $Cl(D_1)$ of the fundamental

discriminant D_1 and to pull the mapped ideal back to the class group $Cl(D)$ of the non-fundamental discriminant D are as follows.

5 Algorithm GoToNonMaxOrder

Input: reduced ideal $(A, B) \in Cl(D_1)$, conductor q

Output: reduced ideal $(a, b) \in Cl(D)$ such that

$(a, b) = \Psi(v)$ where $\Psi: Cl(D_1) \rightarrow Cl(D)$ and

v is an element of $Cl(D)$

- 10 1. $a \leftarrow A$
2. $b \leftarrow Bq \bmod 2a, (-a \leq b < a)$
3. RETURN (a, b)

Algorithm GoToMaxOrder

15 Input: reduced ideal $(a, b) \in Cl(D)$,

 fundamental discriminant D_1 , conductor q

Output: reduced ideal $(A, B) \in Cl(D_1)$ such that

$(A, B) = \Phi(\alpha)$ where $\Phi: Cl(D) \rightarrow Cl(D_1)$ and

α is an element of $Cl(D_1)$

- 20 1. /* Compute $(A, B) = (a, b)O_{D_1}$ */
 - 1.1. $A \leftarrow a$
 - 1.2. $b_0 \leftarrow D \bmod 2$
 - 1.3. Solve $1 = \mu q + \lambda a$ for $\mu, \lambda \in \mathbb{Z}$

using the extended Euclidean algorithm
 - 1.4. $B \leftarrow b\mu + ab_0\lambda \bmod 2a, (-A \leq B < A)$
- 25 2. /* Reduce (A, B) */
 - 2.1. $C \leftarrow (D_1 - B^2)/4A$
 - 2.2. WHILE $\{-A < B \leq A < C\}$ or $\{0 \leq B \leq A = C\}$ DO
 - 2.2.1. Find $\mu, \lambda \in \mathbb{Z}$ such that $-A \leq \mu = B + 2\lambda A < A$

using division with remainder
 - 2.2.2. $(A, B, C) \leftarrow (C - (B + \mu)\lambda/2, \mu, A)$
 - 2.3. IF $A = C$ AND $B < 0$ THEN $B \leftarrow -B$
 - 2.4. RETURN (A, B)
- 30
- 35

In this undeniable digital signature scheme, the

required amount of computations is small so that the signature verification can be done very fast even when the public keys are made very long.

To demonstrate the effectiveness of this undeniable digital signature scheme, this undeniable digital signature scheme and the conventional RSA-type undeniable digital signature scheme were implemented in form of software and the running times of each step in these two schemes were compared, for an exemplary case of using the bit length of the public key equal to 1024 bits. Fig. 5 summarizes the result of this simulation. As can be seen from Fig. 5, the key generation and the signature verification of the undeniable digital signature scheme of the present invention are much faster than those of the conventional RSA-type undeniable digital signature scheme.

Moreover, when the bit length of the public key is doubled, from 1024 bits to 2048 bits for example, the processing time of the undeniable digital signature scheme of the present invention becomes only twice longer, whereas the processing time of the conventional RSA-type undeniable digital signature scheme becomes about eight times longer.

Next, with references to Fig. 6 to Fig. 9, exemplary practical applications of the undeniable digital signature scheme according to the present invention will be described in detail.

Fig. 6 shows a schematic configuration of an undeniable digital signature system for a software vending service, which comprises clients 101 and 102 that are connected to a communication network 108 such as the Internet, and authentication servers 105 and software vending servers 106 that are connected to the communication network 108 through a firewall 109.

In this system, the authentication server 105 issues a secret key of the undeniable signature for the software

vending server 106. The authentication server 105 also attaches a software vendor's undeniable digital signature to each software offered for downloading at the software vending server 106. When the client 101 or 102 downloads
5 the software with the undeniable digital signature attached thereto from the software vending server 106, the client 101 or 102 can prove that the software has not been altered from an original (the software is not infected by any computer virus) by carrying out the process for verifying
10 the undeniable digital signature interactively with the authentication server 105. Thus in this system the client 101 or 102 is the verifier and the authentication server 105 is the signer. In this way, it becomes possible to detect a downloaded software that is infected by any
15 computer virus.

When the undeniable digital signature scheme according to the present invention is used in this system, the authentication server is only required to carry out the verification step II, which can be done very fast as
20 already noted above, so that the processing load on the authentication server can be reduced considerably even in the case of a large scale system.

Furthermore, in the undeniable digital signature scheme of the present invention, a time required for the
25 key generation is about 1 second which is much shorter than about 30 minutes required in the conventional RSA-type digital signature scheme. When the conventional RSA-type digital signature scheme is utilized in signing a large number of different softwares, it has been practically
30 inevitable to use the same key many times because the key generation takes a rather long time. However, this use of the same key many times can be potentially problematic from a viewpoint of the security because, once the key used for one software is attacked somehow, the security of all the
35 softwares for which the same key has been used is also

lost. In this regard, in the undeniable digital signature scheme of the present invention, the key generation takes only a very short time so that there is no need to use the same key many times and it is possible to use each key only once so as to further improve the security.

In the system of Fig. 6, each authentication server can have an exemplary configuration as shown in Fig. 7, in which a network interface 201, a CPU (Central Processing Unit) 202, a main memory 203, an undeniable digital signature key storage area 204, console and display interfaces 205, a secondary memory device 206 such as a magnetic disk device, and a supplementary memory device 207 such as a magneto-optic disk device are interconnected through a bus. Here, the undeniable digital signature key storage area 204 is connected to the bus through an access control circuit 208, and an undeniable digital signature processing program 209 is stored in the secondary memory device 206.

Fig. 8 shows a schematic configuration of an undeniable digital signature system for an e-commerce service.

In recent years, in conjunction with the rapid spread of the e-commerce on the Internet, troubles between customers and e-commerce stores are also increasing. For instance, there is a trouble of a product delivery failure despite of the proper payment made by the customer. In order to eliminate such troubles, it is effective for the e-commerce store to obtain a certificate issued by the trusted certificate authority and give this certificate to the customer at a time of purchase contract. Here, it is suitable to utilize the undeniable signature for the certificate so that the certificate cannot be reused illegally.

In this system of Fig. 8, an e-commerce store 302 makes a certification request to a certificate authority

303 in order to obtain a certificate. In response to this certification request, the certificate authority 303 tests the validity of the e-commerce store 302. If the e-commerce store 302 passes the test, the certificate authority 303
5 generates a pair of secret keys and public keys of a digital signature for the e-commerce store 302. The certificate authority 303 also generates a signature for the public keys using the undeniable digital signature scheme of the present invention, and sends a set of the secret
10 keys, the public keys, and the signature as a certificate to the e-commerce store 302.

Then, before purchasing a product from the e-commerce store 302, a customer 301 checks the authenticity of the e-commerce store 302 as follows. Namely, the customer 301
15 first obtains the public keys and the signature from the e-commerce store 302. Then, the customer 301 makes a store authentication request to the certificate authority 303. In response to this store authentication request, the signature verification of the undeniable digital signature
20 is carried out by the certificate authority 303 as a signer and the customer 301 as a verifier. If the signature verification fails, it implies that the public keys are not authentic ones issued by the certificate authority 303 so that the customer 301 should not trust the e-commerce store
25 302.

On the other hand, if the signature verification succeeds, it implies that the public keys are authentic ones issued by the certificate authority 303. In this case, the customer 301 next generates a random data, encrypts it
30 using the public keys of the e-commerce store 302, and sends the encrypted random data to the e-commerce store 302. In response, the e-commerce store 302 decrypts the encrypted random number using the secret keys of the e-commerce store 302, and returns the decrypted random data
35 to the customer 301. The customer 301 then checks if the

decrypted random data coincides with the original random data. If they coincide, it implies that the e-commerce store 302 also has the authentic secret keys issued by the certificate authority 303 that corresponds to the public
5 keys so that the customer 301 can regard the e-commerce store 302 as trustworthy and make a product purchase from the e-commerce store 302. In this way, it becomes possible to check the authenticity of the e-commerce service provider.

10 The above described procedure may be modified as follows.

Namely, in the system of Fig. 8, the e-commerce store 302 has a home page, and makes a certification request to the certificate authority 303 in order to obtain a
15 certificate of the home page. In response to this certification request, the certificate authority 303 tests the validity of the e-commerce store 302. If the e-commerce store 302 passes the test, the certificate authority 303 generates a signature for the hash value of the home page
20 using the undeniable digital signature scheme of the present invention, and posts the signature as a certificate on the home page of the e-commerce store 302 as displayed on the customer's browser. Here, the certificate is not directly issued to the e-commerce store 302 but made to
25 appear on a display of the home page of the e-commerce store 302 on the customer's browser, so as to prevent an illegal copy of the certificate by the e-commerce store 302.

Then, before purchasing a product from the e-commerce
30 store 302, the customer 301 checks the authenticity of the e-commerce store 302 as follows. Namely, the customer 301 clicks the certificate posted on the home page of the e-commerce store 302. In response, the signature is sent to the customer 301 and the customer 301 is linked to the
35 certificate authority 303. Then, the signature verification

of the undeniable digital signature is carried out by the certificate authority 303 as a signer and the customer 301 as a verifier. If the signature verification fails, it implies that the home page is not authentic one whose hash value is signed by the certificate authority 303 so that the customer 301 should not trust the e-commerce store 302. On the other hand, if the signature verification succeeds, the customer 301 can regard the e-commerce store 302 as trustworthy and make a product purchase from the e-commerce store 302. In this way, it also becomes possible to check the authenticity of the e-commerce service provider.

Fig. 9 shows a schematic configuration of an undeniable digital signature system for a news/mail providing service.

In recent years, there are increasing threats of SPAM mails, a computer virus infection through mails or attached files, and a social disorder due to unreliable news. In order to eliminate such threats, the news/mail provider can attach an undeniable signature to the provided news/mails, such that the recipient can open/read the received news/mails only after checking the authenticity of the provider with the trusted certificate authority.

In this system of Fig. 9, a news/mail provider 402 makes a certification request to a certificate authority 403 in order to obtain a certificate. In response to this certification request, the certificate authority 403 tests the validity of the news/mail provider 402. If the news/mail provider 402 passes the test, the certificate authority 403 generates a pair of secret keys and public keys of a digital signature for the news/mail provider 402. The certificate authority 403 also generates a signature for the public keys using the undeniable digital signature scheme of the present invention, and sends a set of the secret keys, the public keys, and the signature as a certificate to the news/mail provider 402.

Then, before opening news/mails received from the news/mail provider 402, a reader 401 checks the authenticity of the news/mail provider 402 as follows. Namely, the reader 401 first obtains the public keys and
5 the signature from the news/mail provider 402. Then, the reader 401 makes a provider authentication request to the certificate authority 403. In response to this store authentication request, the signature verification of the undeniable digital signature is carried out by the
10 certificate authority 403 as a signer and the reader 401 as a verifier. If the signature verification fails, it implies that the public keys are not authentic ones issued by the certificate authority 403 so that the reader 401 should not trust the news/mail provider 402.

15 On the other hand, if the signature verification succeeds, it implies that the public keys are authentic ones issued by the certificate authority 403. In this case, the reader 401 next generates a random data, encrypts it using the public keys of the news/mail provider 402, and
20 sends the encrypted random data to the news/mail provider 402. In response, the news/mail provider 402 decrypts the encrypted random number using the secret keys of the news/mail provider 402, and returns the decrypted random data to the reader 401. The reader 401 then checks if the
25 decrypted random data coincides with the original random data. If they coincide, it implies that the news/mail provider 402 also has the authentic secret keys issued by the certificate authority 403 that corresponds to the public keys so that the reader 401 can regard the news/mail
30 provider 402 as trustworthy and open the news/mails received from the news/mail provider 402. In this way, it becomes possible to check the authenticity of the information service provider.

The above described procedure may be modified as
35 follows.

Namely, in the system of Fig. 9, the news/mail provider 402 has a home page, and makes a certification request to the certificate authority 403 in order to obtain a certificate of the home page. In response to this
5 certification request, the certificate authority 403 tests the validity of the news/mail provider 402. If the news/mail provider 402 passes the test, the certificate authority 403 generates a signature for the hash value of the home page using the undeniable digital signature scheme
10 of the present invention, and posts the signature as a certificate on the home page of the news/mail provider 402 as displayed on the reader's browser. Here, the certificate is not directly issued to the news/mail provider 402 but made to appear on a display of the home page of the
15 news/mail provider 402 on the reader's browser, so as to prevent an illegal copy of the certificate by the news/mail provider 402.

Then, before opening news/emails received from the news/mail provider 402, the reader 401 checks the
20 authenticity of the news/mail provider 402 as follows. Namely, the reader 401 clicks the certificate posted on the home page of the news/mail provider 402. In response, the signature is sent to the reader 401 and the reader 401 is linked to the certificate authority 403. Then, the
25 signature verification of the undeniable digital signature is carried out by the certificate authority 403 as a signer and the reader 401 as a verifier. If the signature verification fails, it implies that the home page is not authentic one whose hash value is signed by the certificate
30 authority 403 so that the reader 401 should not trust the news/mail provider 402. On the other hand, if the signature verification succeeds, the reader 401 can regard the news/mail provider 402 as trustworthy and open the news/emails received from the news/mail provider 402. In
35 this way, it also becomes possible to check the

authenticity of the e-commerce service provider.

It is to be noted that the above described embodiments according to the present invention may be conveniently
5 implemented using a conventional general purpose digital computer programmed according to the teachings of the present specification, as will be apparent to those skilled in the computer art. Appropriate software coding can readily be prepared by skilled programmers based on the
10 teachings of the present disclosure, as will be apparent to those skilled in the software art.

In particular, each of the signer device and the verifier device of the above described embodiments can be conveniently implemented in a form of a software package.

15 Such a software package can be a computer program product which employs a storage medium including stored computer code which is used to program a computer to perform the disclosed function and process of the present invention. The storage medium may include, but is not
20 limited to, any type of conventional floppy disks, optical disks, CD-ROMs, magneto-optical disks, ROMs, RAMs, EPROMs, EEPROMs, magnetic or optical cards, or any other suitable media for storing electronic instructions.

It is also to be noted that, besides those already
25 mentioned above, many modifications and variations of the above embodiments may be made without departing from the novel and advantageous features of the present invention. Accordingly, all such modifications and variations are intended to be included within the scope of the appended
30 claims.

WHAT IS CLAIMED IS:

1. A method of undeniable digital signature, comprising the steps of:

5 (a) generating public keys (D, P, k, t) and secret keys $(D1, q)$ at a signer side, by generating two primes p, q ($p, q > 4, p = 3 \bmod 4, \sqrt{p/3} < q$), computing $D1 = -p$ and $D = D1q^2$, obtaining a bit length k of $\sqrt{|D1|}/4$ and a bit length t of $q - (D1/q)$ where $(D1/q)$ denotes Kronecker symbol, and
10 generating a kernel element P of a map from a class group $Cl(D)$ to a class group $Cl(D1)$;

(b) generating a signature S for a message m at the signer side, by embedding the message m into a message ideal M in the class group $Cl(D)$ where a norm of the message ideal M
15 is larger than $k+1$ bits, and mapping the message ideal M to the class group $Cl(D1)$ and pulling the mapped message ideal M back to the class group $Cl(D)$; and

(c) verifying the signature S by:

(c1) checking whether a norm $N(S)$ of the signature S
20 is smaller than k bits or not, and judging that the signature S is illegal when the norm $N(S)$ is larger than k bits, or generating a challenge C when the norm $N(S)$ is not larger than k bits, by computing the message ideal M of the message m , generating a random integer r smaller than t
25 bits, computing $H = (M/S)^r$, generating a random ideal B whose norm is smaller than $k-1$ bits, and computing the challenge $C = BH$, at a verifier side;

(c2) computing a response W by mapping the challenge C to the class group $Cl(D1)$ and pulling the mapped challenge
30 C back to the class group $Cl(D)$ and squaring a result of mapping and pulling back, using the secret keys $(D1, q)$, at the signer side; and

(c3) checking whether $W = B^2$ holds or not, and judging that the signature S is legal when $W = B^2$ holds or that the
35 signature S is illegal otherwise, at the verifier side.

2. A signer device for processing an undeniable digital signature, comprising:

a key generation unit for generating public keys (D, P, k, t) and secret keys (D1, q), by generating two primes p, q ($p, q > 4$, $p \equiv 3 \pmod{4}$, $\sqrt{p/3} < q$), computing $D1 = -p$ and $D = D1q^2$, obtaining a bit length k of $\sqrt{|D1|}/4$ and a bit length t of $q - (D1/q)$ where $(D1/q)$ denotes Kronecker symbol, and generating a kernel element P of a map from a class group $Cl(D)$ to a class group $Cl(D1)$;

a signature generation unit for generating a signature S for a message m, by embedding the message m into a message ideal M in the class group $Cl(D)$ where a norm of the message ideal M is larger than k+1 bits, and mapping the message ideal M to the class group $Cl(D1)$ and pulling the mapped message ideal M back to the class group $Cl(D)$; and

a response generation unit for receiving a challenge $C = BH$ from a verifier side, where B is a random ideal whose norm is smaller than k-1 bits, $H = (M/S)^r$, and r is a random integer smaller than t bits, computing a response W by mapping the challenge C to the class group $Cl(D1)$ and pulling the mapped challenge C back to the class group $Cl(D)$ and squaring a result of mapping and pulling back, using the secret keys (D1, q), and sending the response W to the verifier side, in a process for verifying the signature S.

3. A verifier device for processing an undeniable digital signature, using a message m and a signature S received from a signer side, where public keys (D, P, k, t) and secret keys (D1, q) are defined by generating two primes p, q ($p, q > 4$, $p \equiv 3 \pmod{4}$, $\sqrt{p/3} < q$), computing $D1 = -p$ and $D = D1q^2$, obtaining a bit length k of $\sqrt{|D1|}/4$ and a bit length t of $q - (D1/q)$ where $(D1/q)$ denotes Kronecker symbol,

and generating a kernel element P of a map from a class group $Cl(D)$ to a class group $Cl(D_1)$, and the signature S for the message m is generated by embedding the message m into a message ideal M in the class group $Cl(D)$ where a
5 norm of the message ideal M is larger than $k+1$ bits, and mapping the message ideal M to the class group $Cl(D_1)$ and pulling the mapped message ideal M back to the class group $Cl(D)$, the verifier device comprising:

10 a norm checking unit for checking whether a norm $N(S)$ of the signature S is smaller than k bits or not, and judging that the signature S is illegal when the norm $N(S)$ is larger than k bits;

15 a challenge generation unit for generating a challenge C when the norm $N(S)$ is not larger than k bits, by computing the message ideal M of the message m , generating a random integer r smaller than t bits, computing $H = (M/S)^r$, generating a random ideal B whose norm is smaller than $k-1$ bits, and computing a challenge $C = BH$, and for sending the challenge C to a signer side; and

20 a response checking unit for receiving a response W from the signer side, checking whether $W = B^2$ holds or not, and judging that the signature S is legal when $W = B^2$ holds or that the signature S is illegal otherwise, where the response W being obtained by mapping the challenge C to the
25 class group $Cl(D_1)$ and pulling the mapped challenge C back to the class group $Cl(D)$ and squaring a result of mapping and pulling back, using the secret keys (D_1, q) .

4. A computer usable medium having computer readable
30 program codes embodied therein for causing a computer to function as a signer device for processing an undeniable digital signature, the computer readable program codes including:

35 a first computer readable program code for causing said computer to generate public keys (D, P, k, t) and

secret keys $(D1, q)$, by generating two primes p, q ($p, q > 4, p \equiv 3 \pmod{4}, \sqrt{p/3} < q$), computing $D1 = -p$ and $D = D1q^2$, obtaining a bit length k of $\sqrt{|D1|}/4$ and a bit length t of $q - (D1/q)$ where $(D1/q)$ denotes Kronecker symbol, and

- 5 generating a kernel element P of a map from a class group $Cl(D)$ to a class group $Cl(D1)$;

a second computer readable program code for causing said computer to generate a signature S for a message m , by embedding the message m into a message ideal M in the class
10 group $Cl(D)$ where a norm of the message ideal M is larger than $k+1$ bits, and mapping the message ideal M to the class group $Cl(D1)$ and pulling the mapped message ideal M back to the class group $Cl(D)$; and

a third computer readable program code for causing
15 said computer to receive a challenge $C = BH$ from a verifier side, where B is a random ideal whose norm is smaller than $k-1$ bits, $H = (M/S)^r$, and r is a random integer smaller than t bits, compute a response W by mapping the challenge C to the class group $Cl(D1)$ and pulling the mapped
20 challenge C back to the class group $Cl(D)$ and squaring a result of mapping and pulling back, using the secret keys $(D1, q)$, and send the response W to the verifier side, in a process for verifying the signature S .

- 25 5. A computer usable medium having computer readable program codes embodied therein for causing a computer to function as a verifier device for processing an undeniable digital signature, using a message m and a signature S received from a signer side, where public keys (D, P, k, t)
30 and secret keys $(D1, q)$ are defined by generating two primes p, q ($p, q > 4, p \equiv 3 \pmod{4}, \sqrt{p/3} < q$), computing $D1 = -p$ and $D = D1q^2$, obtaining a bit length k of $\sqrt{|D1|}/4$ and a bit length t of $q - (D1/q)$ where $(D1/q)$ denotes Kronecker symbol, and generating a kernel element P of a map from a
35 class group $Cl(D)$ to a class group $Cl(D1)$, and the

signature S for the message m is generated by embedding the message m into a message ideal M in the class group $Cl(D)$ where a norm of the message ideal M is larger than $k+1$ bits, and mapping the message ideal M to the class group
5 $Cl(D_1)$ and pulling the mapped message ideal M back to the class group $Cl(D)$, the computer readable program codes including:

a first computer readable program code for causing said computer to check whether a norm $N(S)$ of the signature
10 S is smaller than k bits or not, and judge that the signature S is illegal when the norm $N(S)$ is larger than k bits;

a second computer readable program code for causing said computer to generate a challenge C when the norm $N(S)$
15 is not larger than k bits, by computing the message ideal M of the message m, generating a random integer r smaller than t bits, computing $H = (M/S)^r$, generating a random ideal B whose norm is smaller than $k-1$ bits, and computing the challenge $C = BH$, and send the challenge C to a signer
20 side; and

a third computer readable program code for causing said computer to receive a response W from the signer side, check whether $W = B^2$ holds or not, and judge that the signature S is legal when $W = B^2$ holds or that the
25 signature S is illegal otherwise, where the response W being obtained by mapping the challenge C to the class group $Cl(D_1)$ and pulling the mapped challenge C back to the class group $Cl(D)$ and squaring a result of mapping and pulling back, using the secret keys (D_1, q) .

30

6. A method for providing a software vending service, comprising the steps of:

(a) attaching an undeniable digital signature to a software offered for downloading by clients at a software
35 vendor side, according to an undeniable digital signature

scheme based on a quadratic field; and

(b) carrying out a process of verifying the undeniable digital signature at the software vendor side interactively with each client which has downloaded the software with the undeniable digital signature attached thereto, so as to prove that the software has not been altered from an original.

7. The method of claim 6, wherein the step (a) further includes the steps of:

(a1) generating public keys (D, P, k, t) and secret keys $(D1, q)$ at the software vendor side, by generating two primes p, q ($p, q > 4, p \equiv 3 \pmod{4}, \sqrt{p/3} < q$), computing $D1 = -p$ and $D = D1q^2$, obtaining a bit length k of $\sqrt{|D1|}/4$ and a bit length t of $q - (D1/q)$ where $(D1/q)$ denotes Kronecker symbol, and generating a kernel element P of a map from a class group $Cl(D)$ to a class group $Cl(D1)$; and

(a2) generating a signature S for a message m representing the software at the software vendor side, by embedding the message m into a message ideal M in the class group $Cl(D)$ where a norm of the message ideal M is larger than $k+1$ bits, and mapping the message ideal M to the class group $Cl(D1)$ and pulling the mapped message ideal M back to the class group $Cl(D)$.

25

8. The method of claim 7, wherein the step (b) further includes the steps of:

(b1) checking whether a norm $N(S)$ of the signature S is smaller than k bits or not, and judging that the signature S is illegal when the norm $N(S)$ is larger than k bits, or generating a challenge C when the norm $N(S)$ is not larger than k bits, by computing the message ideal M of the message m , generating a random integer r smaller than t bits, computing $H = (M/S)^r$, generating a random ideal B whose norm is smaller than $k-1$ bits, and computing the

challenge $C = BH$, at a client side;

(b2) computing a response W by mapping the challenge C to the class group $Cl(D1)$ and pulling the mapped challenge C back to the class group $Cl(D)$ and squaring a result of mapping and pulling back, using the secret keys $(D1, q)$, at the software vendor side; and

(b3) checking whether $W = B^2$ holds or not, and judging that the signature S is legal when $W = B^2$ holds or that the signature S is illegal otherwise, at the client side.

10

9. The method of claim 6, wherein the step (a) attaches the undeniable digital signature using different sets of public keys and secret keys for different softwares.

15 10. A method for enabling a user to check authenticity of an e-commerce/information service provider, comprising the steps of:

(a) obtaining public keys, secret keys, and a signature for the public keys from a certificate authority at the e-commerce/information service provider, the signature being generated by the certificate authority according to an undeniable digital signature scheme;

(b) providing the public keys and the signature from the e-commerce/information service provider to the user, such that the user carries out a process of verifying the signature provided from the e-commerce/information service provider to the user, interactively with the certificate authority to prove authenticity of the public keys provided by the e-commerce/information service provider; and

(c) receiving an encrypted random data from the user, the encrypted random data being encrypted by the user using the public keys, decrypting the encrypted random data using the secret keys, and returning a decrypted random data to the user, such that the user checks if the decrypted random data coincides with an original random data to prove that

the e-commerce/information service provider has authentic secret keys.

11. The method of claim 10, wherein at the step (a) the signature is generated according to an undeniable digital signature scheme based on a quadratic field.

12. The method of claim 11, wherein at the step (a) the public keys, the secret keys, and the signature are generated by the steps of:

(a1) generating the public keys (D, P, k, t) and the secret keys $(D1, q)$ at the certificate authority, by generating two primes p, q ($p, q > 4, p \equiv 3 \pmod{4}, \sqrt{p/3} < q$), computing $D1 = -p$ and $D = D1q^2$, obtaining a bit length k of $\sqrt{|D1|}/4$ and a bit length t of $q - (D1/q)$ where $(D1/q)$ denotes Kronecker symbol, and generating a kernel element P of a map from a class group $Cl(D)$ to a class group $Cl(D1)$; and

(a2) generating the signature S for the public keys at the certificate authority, by embedding the public keys into a message ideal M in the class group $Cl(D)$ where a norm of the message ideal M is larger than $k+1$ bits, and mapping the message ideal M to the class group $Cl(D1)$ and pulling the mapped message ideal M back to the class group $Cl(D)$.

13. The method of claim 12, wherein at the step (b) the signature is verified by the steps of:

(b1) checking whether a norm $N(S)$ of the signature S is smaller than k bits or not, and judging that the signature S is illegal when the norm $N(S)$ is larger than k bits, or generating a challenge C when the norm $N(S)$ is not larger than k bits, by computing the message ideal M of the public keys, generating a random integer r smaller than t bits, computing $H = (M/S)^r$, generating a random ideal B whose norm is smaller than $k-1$ bits, and computing the challenge

C = BH, at a user side;

(b2) computing a response W by mapping the challenge C to the class group Cl(D1) and pulling the mapped challenge C back to the class group Cl(D) and squaring a result of mapping and pulling back, using the secret keys (D1, q), at a certificate authority side; and

(b3) checking whether $W = B^2$ holds or not, and judging that the signature S is legal when $W = B^2$ holds or that the signature S is illegal otherwise, at the user side.

10

14. A method for enabling a user to check authenticity of an e-commerce/information service provider, comprising the steps of:

(a) issuing public keys, secret keys, and a signature for the public keys from a certificate authority to the e-commerce/information service provider, the signature being generated according to an undeniable digital signature scheme; and

(b) carrying out a process of verifying the signature provided from the e-commerce/information service provider to the user, at the certificate authority interactively with the user in order to prove authenticity of the public keys provided by the e-commerce/information service provider.

25

15. The method of claim 14, wherein at the step (a) the signature is generated according to an undeniable digital signature scheme based on a quadratic field.

30 16. The method of claim 15, wherein at the step (a) the public keys, the secret keys, and the signature are generated by the steps of:

(a1) generating the public keys (D, P, k, t) and the secret keys (D1, q) at the certificate authority, by generating two primes p, q ($p, q > 4$, $p \equiv 3 \pmod{4}$, $\sqrt{p/3} <$

q), computing $D1 = -p$ and $D = D1q^2$, obtaining a bit length k of $\sqrt{|D1|}/4$ and a bit length t of $q - (D1/q)$ where $(D1/q)$ denotes Kronecker symbol, and generating a kernel element P of a map from a class group $Cl(D)$ to a class group $Cl(D1)$;

5 and

(a2) generating the signature S for the public keys at the certificate authority, by embedding the public keys into a message ideal M in the class group $Cl(D)$ where a norm of the message ideal M is larger than $k+1$ bits, and mapping
10 the message ideal M to the class group $Cl(D1)$ and pulling the mapped message ideal M back to the class group $Cl(D)$.

17. The method of claim 16, wherein at the step (b) the signature is verified by the steps of:

15 (b1) checking whether a norm $N(S)$ of the signature S is smaller than k bits or not, and judging that the signature S is illegal when the norm $N(S)$ is larger than k bits, or generating a challenge C when the norm $N(S)$ is not larger than k bits, by computing the message ideal M of the public
20 keys, generating a random integer r smaller than t bits, computing $H = (M/S)^r$, generating a random ideal B whose norm is smaller than $k-1$ bits, and computing the challenge $C = BH$, at a user side;

(b2) computing a response W by mapping the challenge C to
25 the class group $Cl(D1)$ and pulling the mapped challenge C back to the class group $Cl(D)$ and squaring a result of mapping and pulling back, using the secret keys $(D1, q)$, at a certificate authority side; and

(b3) checking whether $W = B^2$ holds or not, and judging
30 that the signature S is legal when $W = B^2$ holds or that the signature S is illegal otherwise, at the user side.

18. A method for enabling a user to check authenticity of an e-commerce/information service provider, comprising the
35 steps of:

(a) generating a signature for a hash value of a home page of the e-commerce/information service provider at a certificate authority according to an undeniable digital signature scheme;

5 (b) posting the signature on a display of the home page of the e-commerce/information service provider at a user side from the certificate authority, such that the user can initiate a process of verifying the signature by clicking the signature on the display; and

10 (c) carrying out the process of verifying the signature at the certificate authority interactively with the user in order to prove authenticity of the e-commerce/information service provider.

15 19. The method of claim 18, wherein at the step (a) the signature is generated according to an undeniable digital signature scheme based on a quadratic field.

20 20. The method of claim 19, wherein at the step (a) the signature are generated by the steps of:

(a1) generating a public keys (D, P, k, t) and a secret keys $(D1, q)$ at the certificate authority, by generating two primes p, q ($p, q > 4, p \equiv 3 \pmod{4}, \sqrt{p/3} < q$), computing $D1 = -p$ and $D = D1q^2$, obtaining a bit length k of $\sqrt{|D1|}/4$ and a bit length t of $q - (D1/q)$ where $(D1/q)$ denotes Kronecker symbol, and generating a kernel element P of a map from a class group $Cl(D)$ to a class group $Cl(D1)$; and

25 (a2) generating the signature S for the hash value of the home page at the certificate authority, by embedding the hash value of the home page into a message ideal M in the class group $Cl(D)$ where a norm of the message ideal M is larger than $k+1$ bits, and mapping the message ideal M to the class group $Cl(D1)$ and pulling the mapped message ideal M back to the class group $Cl(D)$.

35

21. The method of claim 20, wherein at the step (c) the signature is verified by the steps of:

(c1) checking whether a norm $N(S)$ of the signature S is smaller than k bits or not, and judging that the signature
5 S is illegal when the norm $N(S)$ is larger than k bits, or generating a challenge C when the norm $N(S)$ is not larger than k bits, by computing the message ideal M of the public keys, generating a random integer r smaller than t bits, computing $H = (M/S)^r$, generating a random ideal B whose
10 norm is smaller than $k-1$ bits, and computing the challenge $C = BH$, at the user side;

(c2) computing a response W by mapping the challenge C to the class group $Cl(D1)$ and pulling the mapped challenge C back to the class group $Cl(D)$ and squaring a result of
15 mapping and pulling back, using the secret keys $(D1, q)$, at a certificate authority side; and

(c3) checking whether $W = B^2$ holds or not, and judging that the signature S is legal when $W = B^2$ holds or that the signature S is illegal otherwise, at the user side.

20

25

30

35

ABSTRACT OF THE DISCLOSURE

An efficient undeniable digital signature scheme based on a quadratic field is disclosed. Public keys (D, P, k, t) and secret keys $(D1, q)$ are defined by generating two primes p, q ($p, q > 4, p \equiv 3 \pmod{4}, \sqrt{p/3} < q$), computing $D1 = -p$ and $D = D1q^2$, obtaining a bit length k of $\sqrt{|D1|}/4$ and a bit length t of $q - (D1/q)$ where $(D1/q)$ denotes Kronecker symbol, and generating a kernel element P of a map from a class group $Cl(D)$ to a class group $Cl(D1)$. Then the signature verification is realized by first checking whether a norm $N(S)$ of the signature S is smaller than k bits or not, and judging that the signature S is illegal when the norm $N(S)$ is larger than k bits, or generating a challenge C when the norm $N(S)$ is not larger than k bits, by computing the message ideal M of the message m , generating a random integer r smaller than t bits, computing $H = (M/S)^r$, generating a random ideal B whose norm is smaller than $k-1$ bits, and computing the challenge $C = BH$, at a verifier side; then computing a response W by mapping the challenge C to the class group $Cl(D1)$ and pulling the mapped challenge C back to the class group $Cl(D)$ and squaring a result of mapping and pulling back, using the secret keys $(D1, q)$, at the signer side; and then checking whether $W = B^2$ holds or not, and judging that the signature S is legal when $W = B^2$ holds or that the signature S is illegal otherwise, at the verifier side.

30

35

FIG.1

Z	integer ring
D_1	fundamental discriminant($D_1=-p$, $p=3 \bmod 4$, p :prime)
q	conductor(q :prime)
D	non-fundamental discriminant($D=D_1q^2$)
O_D	quadratic order with discriminant $D(O_D=Z+(D+\sqrt{D})/2Z)$
$Cl(D)$	class group with discriminant D
A	ideal in $Cl(D)$ ($A=(a, b)$)
$N(A)$	norm of ideal $A(N(A)=a, A=(a, b))$

FIG.2

Undeniable digital signature scheme of the present invention	
Secret keys	Fundamental discriminant D_1 , conductor q
Public keys	Kernel element P , non-fund. discriminant D
Message	Message ideal M
Signature	$S=GoToNonMaxOrder(GoToMaxOrder(M))$
Verification step 1 (verifier)	$C=BH$, ($H=(M/S)^r$, $r < q$)
Verification step 2 (signer)	$W=(GoToNonMaxOrder(GoToMaxOrder(C)))^2$
Verification step 3 (verifier)	Check $W=B^2$

FIG.3

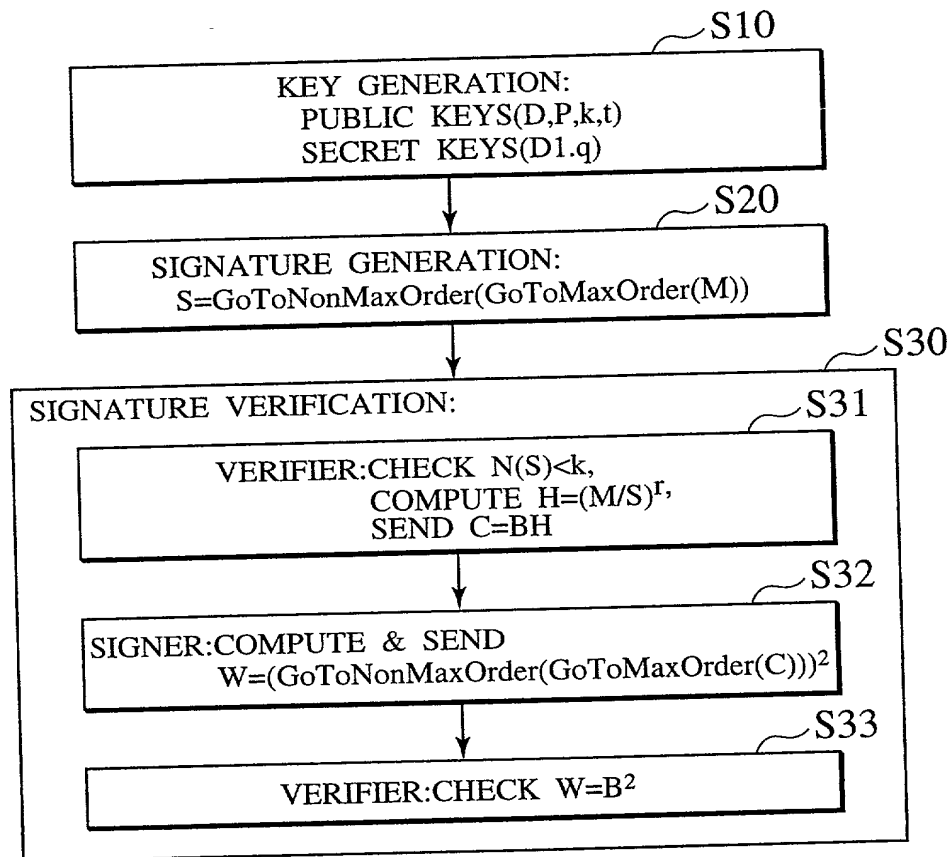


FIG.4

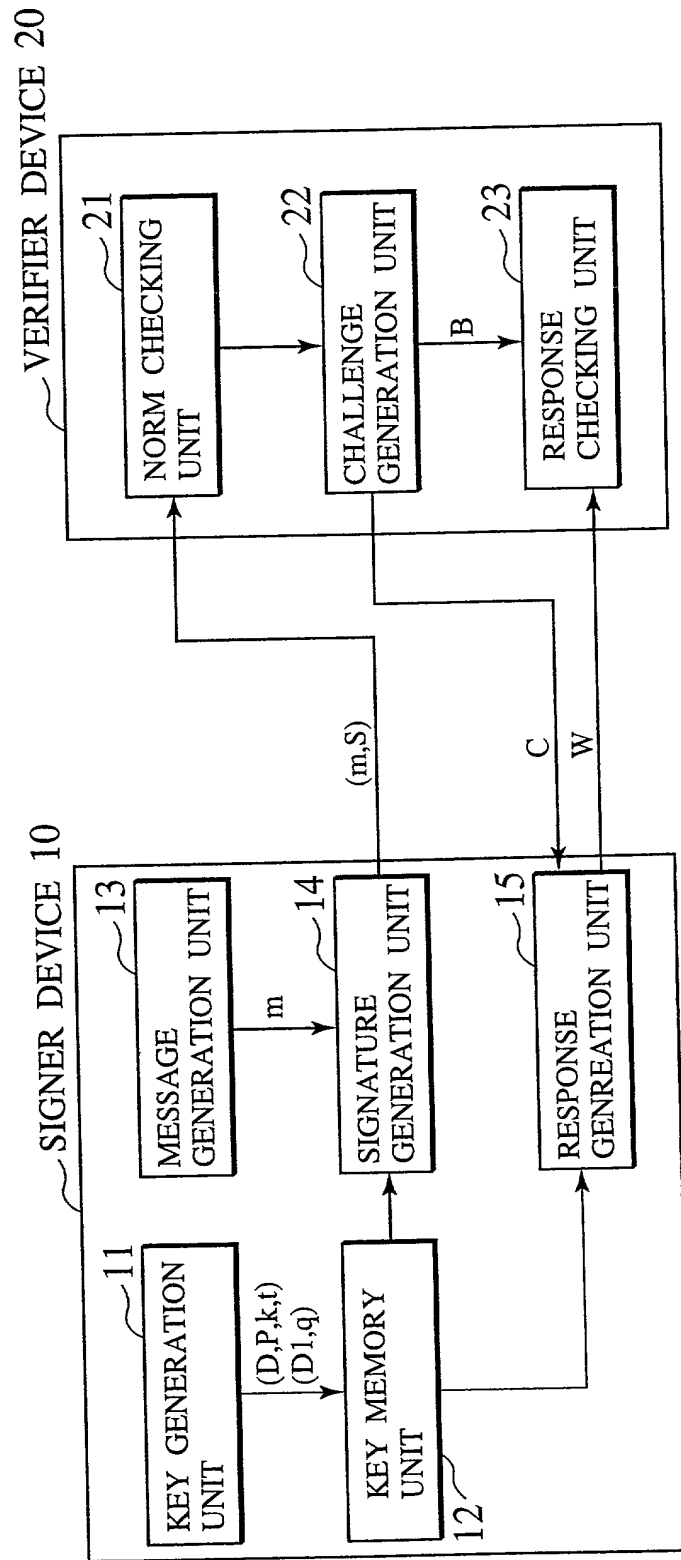


FIG.5

Undeniable digital signature scheme of the present invention		
Key generation	Fund. Disc. DL, conductor q	1360.9ms
	Kernel element P, non-fund. Disc. D	9.0ms
Message embedding	Message ideal M	110.4ms
Signature generation	$S = \text{GoToNonMaxOrder}(\text{GoToMaxOrder}(M))$	1.9ms
Verifier Step 1(verifier)	$C = \text{BH}, (H = (M/S)^r, r < q)$	2083.4ms
Verifier Step 2(signer)	$W = (\text{GoToNonMaxOrder}(\text{GoToMaxOrder}(C)))^2$	7.7ms
Verifier Step 3(verifier)	Check $W = B^2$	4.2ms
Conventional RSA-type undeniable digital signature scheme		
Key generation	$p, q, (p < q, p = 2p' + 1, q = 2q' + 1)$	(42min.)
	$n, e, d, w, S_w (S_w = w^d \bmod n)$	178.4ms
Message embedding	Generation of message m	0.0ms
Signature generation	$S_m = m^d \bmod n$	177.2ms
Verifier Step 1(verifier)	$Q = S_m^i S_w^j \bmod n (i, j \in \mathbb{Z}/n\mathbb{Z})$	350.2ms
Verifier Step 2(signer)	$A = Q^e \bmod n$	177.9ms
Verifier Step 3(verifier)	Check $A = m^{i w^j} \bmod n$	349.6ms

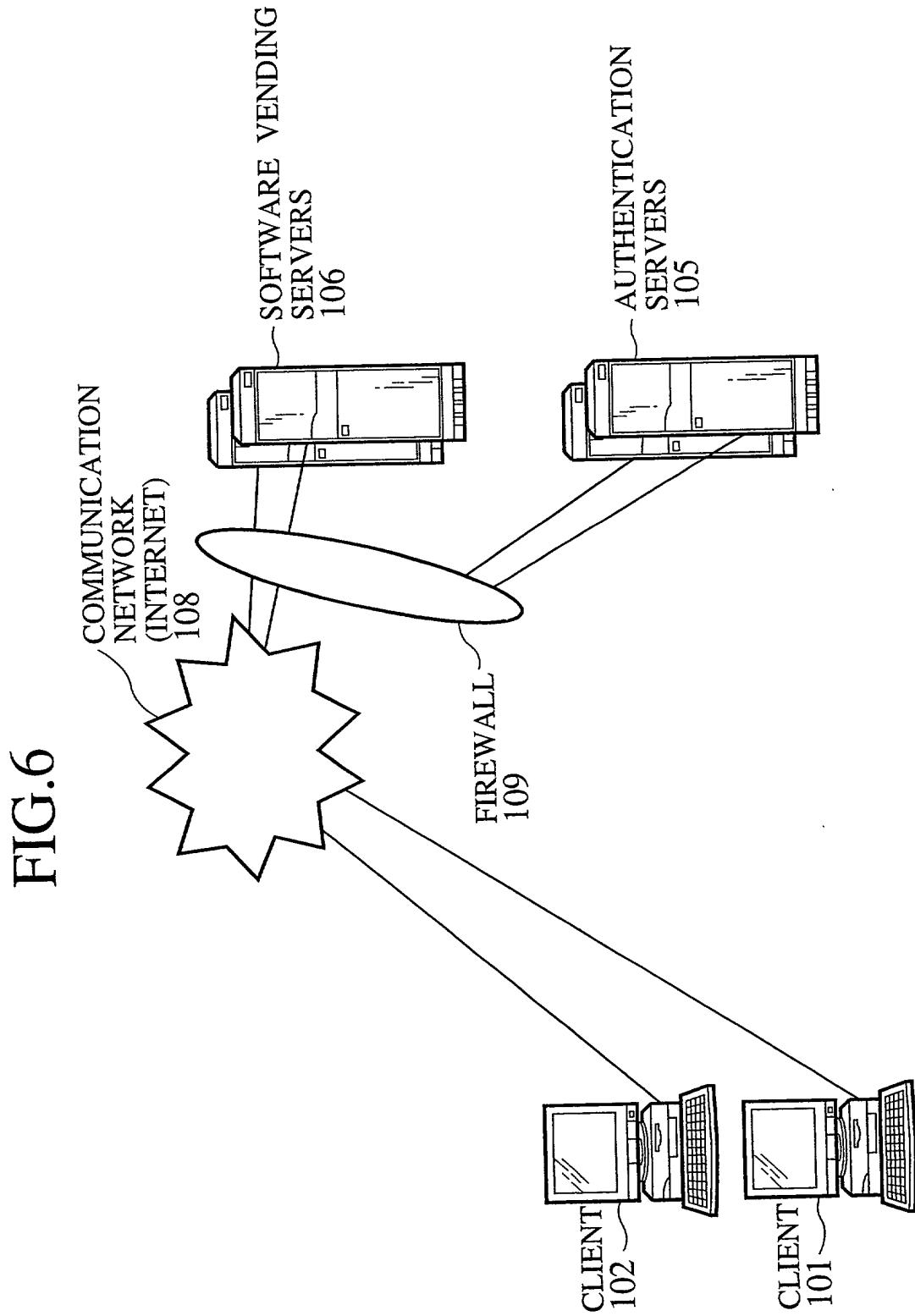


FIG.6

FIG. 7

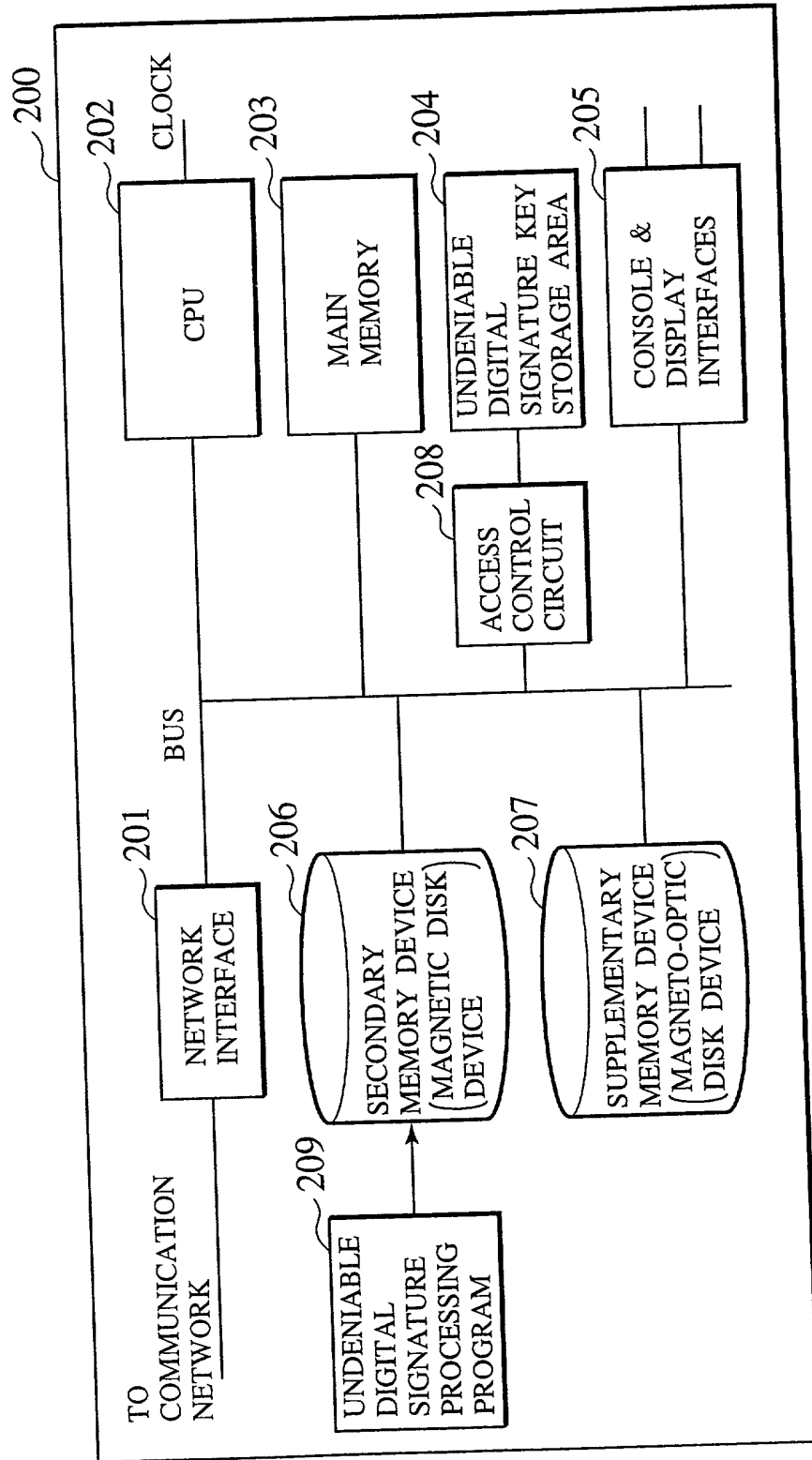
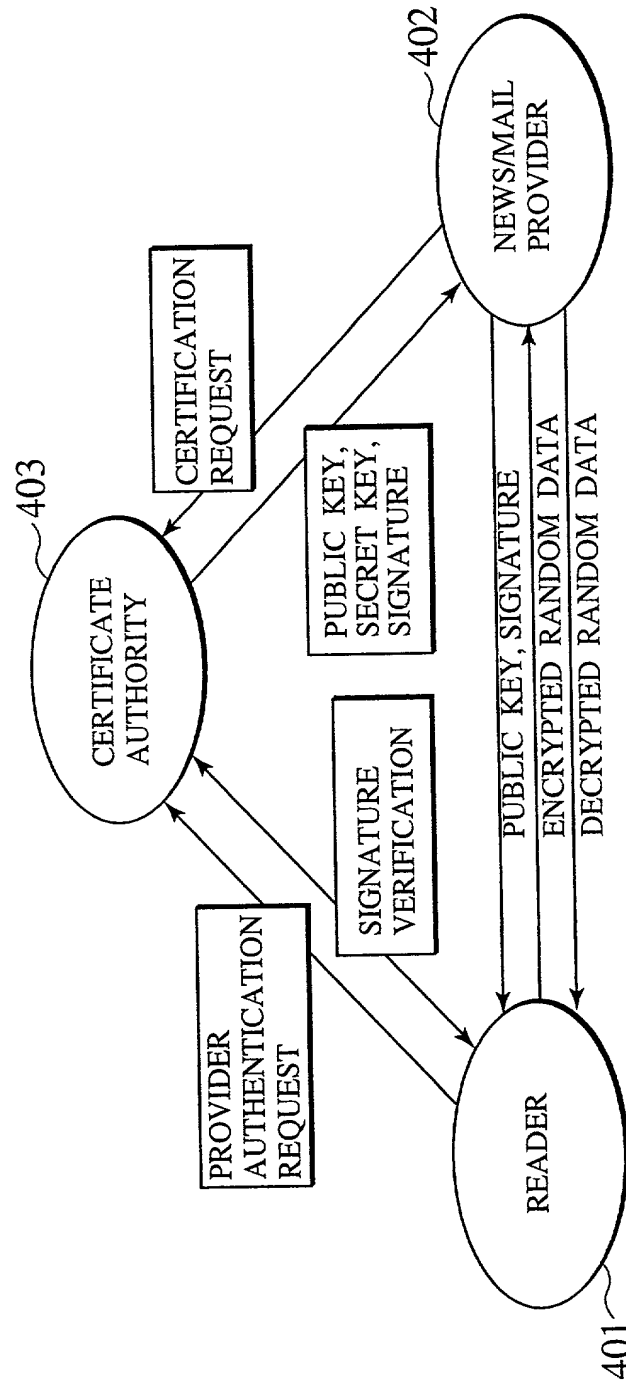


FIG. 9



DECLARATION AND POWER OF ATTORNEY

Attorney's Docket No. 13700-0251

As a below named inventor, I hereby declare that:

My residence, post office address and citizenship are as stated below next to my name. I believe I am the original, first and sole inventor (if only one name is listed below) or an original, first and joint inventor (if plural names are listed below) of the subject matter which is claimed and for which a patent is sought on the invention entitled: _____

UNDENIABLE DIGITAL SIGNATURE SCHEME BASED ON QUADRATIC FIELD, the specification of which

☒ is attached hereto.

☐ was filed on _____ as application Serial No. _____ (if applicable) and was amended on _____.

I hereby state that I have reviewed and understand the contents of the above-identified specification, including the claims, as amended by any amendment referred to above. I do not know and do not believe that the same was ever known or used by others in the United States of America before my or our invention thereof, or patented or described in any printed publication in any country before my or our invention thereof or more than one year prior to the date of this application. I further state that the invention was not in public use or on sale in the United States of America more than one year prior to the date of this application. *I understand that I have a duty of candor and good faith toward the Patent and Trademark Office*, and I acknowledge the duty to disclose information which is material to the examination of this application in accordance with Title 37, Code of Federal Regulations, §1.56(a). I further understand that information is "material" where there is a substantial likelihood that a reasonable patent examiner would consider the information important in deciding whether to allow the application to issue as a patent.

I hereby claim foreign priority benefits under Title 35, United States Code, §119 of my foreign application(s) for patent or inventor's certificate listed below, and have also identified below any foreign application for patent or inventor's certificate disclosing subject matter in common with the above-identified specification and having a filing date before that of the application on which priority is claimed:

Country	App. No.	Date of Filing	Priority Claimed Under 35 USC §119
			Yes _____ No _____

I hereby claim the benefit under Title 35, United States Code, §120 of any United States application(s) listed below and, insofar as the subject matter of each of the claims of this application is not disclosed in the prior United States application in the manner provided by the first paragraph of Title 35, United States Code §112, I acknowledge the duty to disclose material information as defined in Title 37, Code of Federal Regulations, §1.56(a) which occurred between the filing date of the prior application and the national or PCT international filing date of this application:

Application Serial No.	Filing Date	Status: patented, pending, abandoned

I further declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code, and that such willful false statements may jeopardize the validity of the application or any patents issuing thereon.

I hereby authorize the U.S. attorneys named herein to accept and follow instructions from Miyoshi & Miyoshi, as to any action to be taken in the Patent and Trademark Office regarding this application, without direct communication between the U.S. attorney and the undersigned. In the event of a change in the persons from whom instructions may be taken, the U.S. attorney named herein will be notified by the undersigned.

POWER OF ATTORNEY: The following attorneys are hereby appointed to prosecute this application and transact all business in the Patent and Trademark Office connected therewith: Anthony B. Askew - 24,154; Roger T. Frost - 22,176; Jeffrey E. Young - 28,490; Robert E. Richards - 29,105; John R. Harris - 30,388; Stephen M. Schaezel - 31,418; Larry A. Roberts - 31,871; Thomas A. Hodge - 22,602; Charles L. Warner II - 32,320; Gregory T. Gronholm - 32,415; Dale Lischer - 28,438; Peter G. Pappas - 33,205; James Dean Johnson - 31,771; Nora M. Tocups - 35,717; W. Scott Petty - 35,645; Daniel J. Warren - 34,272; Hubert J. Barnhardt III - 36,739; Virginia L. Carron - 37,110; Leona G. Young - 37,266; Jamie L. Greene - 32,467; William A. Hartselle - 36,548; Holmes J. Hawkins III - 38,913; Mary Anthony Merchant - 39,771; Michael J. Mehrman - 40,086; William L. Warren - 36,714; Felipe J. Farley - 38,445; F. Leslie Bessenger III - 39,108; James A. Witherspoon - 36,723; Brenda M. Ozaki - 40,339; James D. Withers - 40,376; M. Todd Mitchem - P40,731; Gregory S. Smith - P40 819

Kilpatrick Stockton LLP

Send correspondence to: 2400 March Tower, 3424 Peachtree Road,
N.E. Atlanta, Georgia 30326

Direct telephone calls (404)949-2400 to:

Roger T. Frost

Full name of solo or first inventor:	Tsuyoshi TAKAGI
Citizenship:	Japan
Residence:	Hansaallee 103, D-40549, Duesseldorf, Germany
Post Office Address:	c/o NIPPON TELEGRAPH AND TELEPHONE CORPORATION 20-2, Nishi-Shinjuku 3-chome, Shinjuku-ku, Tokyo 163-1419 Japan
Inventor's signature	Tsuyoshi Takagi Date: August 28, 2000

☒ Additional inventors are being named on separately numbered sheets attached hereto.

